AXONIUS

Solving the Top Cybersecurity Asset Management Challenges

White Paper • January 2020

Table of Contents.

INTRODUCTION. 3

- OVERVIEW 3
- DEFINING MODERN ASSET MANAGEMENT 3

MODERN ASSET MANAGEMENT TRENDS 4

- MORE CONNECTED DEVICES 4
- MORE SECURITY SOLUTIONS 4
- LACK OF DEDICATED RESOURCES 4

TOP ASSET MANAGEMENT CHALLENGES. 5

- #1 AGGREGATING DATA FROM MANY SECURITY TOOLS 5
- #2 FINDING UNMANAGED DEVICES ON A NETWORK 5
- #3 REAL-TIME INVENTORYING AT MASSIVE SCALE 6
- #4 TESTING COMPLIANCE 6
- #5 DOING MORE WITH LESS 6

CHECKLIST FOR SUCCESSFUL ASSET MANAGEMENT 7

CONCLUSION. 7

FOOTNOTES. 7

ABOUT AXONIUS. 8

Introduction.

Overview

Today, security professionals face many challenges in cybersecurity asset management, from aggregating disparate data sets to establishing real-time visibility in a fluid environment. Emerging technology, such as IoT deployments, and workplace modernization like BYOD continue to complicate this situation. Organizations must understand the depth and breadth of the devices on their network.

In this white paper, you'll learn:

- The 3 trends that are shaping the future of cybersecurity and asset management
- The top 5 challenges to consider when approaching asset management
- The 6 steps you can take to successfully manage your company's assets

Defining Modern Asset Management

As mentioned in a previous white paper titled, "Why Does Asset Management Matter for Cybersecurity?", we defined Cybersecurity Asset Management or "Modern Asset Management" as the process of:

- Gathering data from any source that provides detailed information about assets
- Correlating that data to produce a view of every asset and what is on it
- Continually validating every asset's adherence to the overall security policy
- Creating automatic, triggered actions whenever an asset deviates from the policy

In this context, we will refer to Modern Asset Management as the nexus for cybersecurity projects and decisions.

Modern Asset Management Trends.

Three converging, broad trends are shaping the future of modern asset management as we know it: more connected devices, more security solutions, and lack of dedicated resources.

More Connected Devices

Both the number and types of devices companies are responsible for are dramatically increasing. Cisco IBSG (Internet Business Solutions Group) predicts that there will be **50 billion** devices connected to the internet by 2020[1]. That's nearly 7 connected devices per person, if you divide 50 billion by an estimated 7.6 billion people on Earth in 2020.

The bring-your-own-device (BYOD) era enables people to seamlessly work across company laptops to mobile phones and personal machines while creating complexity for information security teams looking to understand the breadth and depth of their IT asset inventories.

More Security Solutions

One might say, "With great power comes great responsibility.[2]" We say, "With more connected devices come great responsibility." As the number of connected devices continues to rise, so will the *number of solutions* security teams will need to buy to manage them.

451 Research's *Voice of the Enterprise* survey reported that **87%** of companies will see information security spending increase in the year ahead[3]. It's no surprise to see security spending increase as the number of devices within organizations continues to increase.

Lack of Dedicated Resources

The two trends above demonstrate a future of "more" – that is, more devices and more security solutions. One area that does not grow as linearly is internal information security resources. With the number and complexity of information security projects to tackle, companies simply don't have any full-time equivalent (FTE) to spare to dedicate to the management of all these security solutions and devices. In the same 451 Research survey above, **2/3** of enterprises say they don't have enough information security personnel at their organizations[3].

Top Asset Management Challenges.

#1	Aggregating Data from Many Security Tools
#2	Finding Unmanaged Devices on a Network
#3	Real-Time Inventorying at Massive Scale
#4	Testing Compliance
#5	Doing More with Less

#1 Aggregating Data from Many Security Tools

A common scenario, including one we have experienced first-hand, is when a new CISO joins a company and aims to bolster the cybersecurity program by adopting a wide-ranging set of best in class solutions. The challenge lies in efficiently aggregating disparate, enterprise-wide data to understand if security solutions are deployed appropriately and if users have correct permissions.

How To Solve This Challenge

- ❑ Aggregate disparate data sets from different tools
- ❑ Correlate the disparate data to understand depth and context
- ❑ Leverage this actionable information to enforce security policy

#2 Finding Unmanaged Devices on a Network

Oftentimes, a company needs to find unmanaged devices on their network. To illustrate, take this real-life scenario: a financial firm acquires another firm and now needs to migrate new devices onto the privileged network at scale, with a small IT team. The challenge here is finding both new and existing devices that should have a specific security agent or other endpoint agent, but don't.

How To Solve This Challenge

- ❑ Connect to an agent's admin console to see devices with agents
- ❑ Connect to an IAM solution that authenticates and authorizes devices
- ❑ Correlate the data to see which devices are missing endpoint agents

#3 Real-Time Inventorying at Massive Scale

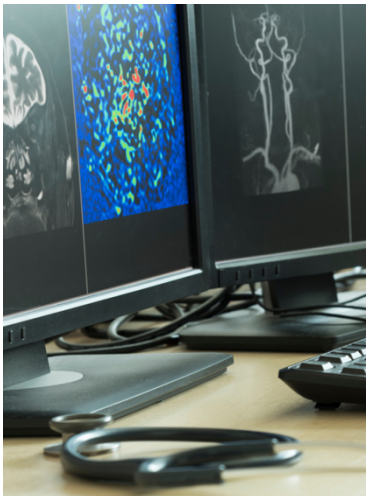
As enterprises scale, so do the breadth and depth of information security challenges. An example of this can be seen in a large, multinational company looking to democratize data for regional IT teams by creating a unified view that inventories and correlates asset data. In this scenario, the challenge is tracking assets accurately – and quickly – in an environment made more complex by regional, siloed IT teams, and complex R&D.

How To Solve This Challenge

- ❑ Connect all security tools to a single aggregator
- ❑ Correlate data across tools in a unified, real-time view
- ❑ Empower IT teams to make decisions for their respective regions

#4 Testing Compliance

One cybersecurity asset management challenge seen in highly regulated industries like healthcare and finance involves testing and managing procedures to ensure compliance. One illustration can be seen with a public healthcare company that performs monthly red team exercises to verify that all devices are compliant with security and software license management policies. Given the frequency of their red team exercises, the challenge presented by this scenario is how to quickly and automatically validate that solutions are deployed appropriately.



How To Solve This Challenge

- ❑ Aggregate device information from Active Directory
- ❑ Determine common security solution coverage gaps
- ❑ Automate policy validation and enforcement

#5 Doing More with Less

Lastly, almost any organization can relate to the scenario of trying to keep up with the number of devices on their network, a challenge made more complex by rapid cloud, BYOD, and IoT adoption. Here, a team must look to eliminate manual, time-consuming tasks by setting cybersecurity asset management on autopilot, which would in turn free up resources to focus on other high-impact projects.

How To Solve This Challenge

- ❑ Aggregate disparate data sets from different tools
- ❑ Determine common security solution coverage gaps
- ❑ Automate policy validation and enforcement
- ❑ Enable teams to make decisions for their respective regions

Checklist for Successful Asset Management.

- ❑ Know which assets are unmanaged
- ❑ Know which managed assets are missing agents
- ❑ Discover new devices automatically
- ❑ Correlate and query vast amounts of data from disparate sources
- ❑ Quickly understand context and detail
- ❑ Develop consistency in communication and issue resolution

Conclusion.

As the number of devices and solutions continue to explode given the trends in BYOD and IoT, so will the breadth and complexity of modern asset management challenges. Enterprises currently have a vast array of security solutions at their disposal to help solve diverse security challenges, but the resources to manage those solutions do not grow as linearly. The forthcoming challenge we anticipate is how security teams can efficiently, credibly, and automatically manage those security solutions.

Footnotes.

1. Cisco, Internet Business Solutions Group, The Internet of Things: How the Next Evolution of the Internet Is Changing Everything, April 2011, Report
2. Peter Parker Principle, A proverb popularized by the Spider-Man comic books written by Stan Lee, Wikipedia
3. 451 Research, Voice of the Enterprise: Information Security, Budgets & Outlook, Published Q1 2019, Report

About Axonius.

Axonius is the cybersecurity asset management platform that gives organizations a comprehensive asset inventory, uncovers security solution coverage gaps, and automatically validates and enforces security policies. By seamlessly integrating with over 200 security and management solutions, Axonius is deployed in minutes, improving cyber hygiene immediately.

Covering millions of devices at customers like the New York Times, Schneider Electric, Landmark Health, AppsFlyer, and many more, Axonius was named the Most Innovative Startup of 2019 at the prestigious RSAC Innovation Sandbox and was named to the CNBC Upstart 100 list and Forbes 20 Rising Stars.

For more information, please visit Axonius.com.